UNITED STATES ENVIRONMENTAL PROTECTION AGENCY
OFFICE OF THE INSPECTOR GENERAL
OFFICE OF INVESTIGATIONS
1200 PENNSYLVANIA AVENUE NW
ARLINGTON, VA 20460

REFERRED FOR ACTION REPORT OF INVESTIGATION CONCERNING

UNKNOWN SUBJECT: IP (b) (7)(E) (EXTERNAL FIREWALL (b) (7)(E))
2009-CS-0145

TABLE OF CONTENTS

Distribution:
[redacted]
DAIGI
STEPHEN NESBITT,
AIGI

Approvals:

_____
Special Agent

_____
Special Agent in Charge

OFFICE OF INSPECTOR GENERAL
OFFICE OF INVESTIGATIONS

CASE NO.:	2009-CS-0145	**DATE OPENED:**	09/24/2009
CASE TITLE:	UNKNOWN SUBJECT: IP (b) (7)(E) (EXTERNAL FIREWALL (b) (7)(E)	**CASE AGENT:**	[redacted]
CASE CATEGORY:	COMPUTER INTRUSION	**OFFICE:**	OFFICE OF INVESTIGATIONS - NERC PHILADELPHIAEASTERN RESOURCE CENTER
JOINT AGENCIES:	None		
JURISDICTION:	MARYLAND		

SECTION A - NARRATIVE

Predication

On August 13, 2009 the Environmental Protection Agency (EPA), Office of the Inspector General (OIG), Office of Investigations (OI) received notification from [redacted] Computer Sciences Corporation (CSC) of an intrusion detected on the EPA's (b) (7)(E) application development site.

Investigation revealed that an alert was detected by the CSC (b) (7)(E) on August 12, 2009 at 4:00PM. An intrusion was detected from several IP addresses with up to10,000 outbound events noted from one single system. In depth review of the CSC (b) system reports revealed unidentified attackers had made 10776 attempts to exploit a (b) (7)(E) [redacted] The CSC (b) detected inbound connection attempts from multiple Internet Protocol (IP) addresses (b) (7)(E)

Possible violations:

1. TITLE 18 USC SEC 1030, Fraud and related activity in connection with computers
2. TITLE 18 USC SEC 1029, Fraud and related activity in connection with access devices

Impact/Dollar Loss

No dollar loss; Potential threat & vulnerability to EPA Information Exchange Network; Flawed & vulnerable testing procedures, No due diligence

Synopsis

Investigation and forensic analysis revealed an intrusion was detected which targeted several Agency systems utilized by CSC to perform testing of [redacted] applications. These systems were created, maintained and operated as a developmental network by CSC within their corporate network. Verification was obtained that no CBI or other sensitive data was available to the intruders on the systems compromised. The entire severity and impact was not determined based on the limited availability and destruction of digital evidence for analysis.

During review of the CSC [(b) (7)] system reports it was noted unidentified attackers had made 10776 attempts [(b) (7)(E)] Subsequent reviews of [(b) (7)(E)] [redacted]

Details

Allegation 1: TITLE 18 USC SEC 1030, Fraud and related activity in connection with computers

Allegation 1 Findings: Forensic analysis and review of CSC [(b) (7)] revealed numerous inbound connection attempts [(b) (7)(E)] [redacted] [(b) (5), (b) (7)(E)] [redacted] nvestigation failed to identify individuals who penetrated the CSC [redacted] test network and systems.

Allegation 2: TITLE 18 USC SEC 1029, Fraud and related activity in connection with access devices

Allegation 2 Findings: Forensic analysis and review of [(b) (7)(E)] [redacted] [(b) (5), (b) (7)(E)] [redacted]. Investigation failed to identify individuals who compromised system access devices for the CSC [redacted] test network and systems.

Disposition

During the course of investigation it was discovered that the intrusion occurred against the CSC company domain where they were testing a [redacted] upgrade. During the early phase of the investigation the contract was transferred to CGI federal for continued execution. In that transition data and systems transferred to CGI federal were unrecoverable. (b) (7)(E) [redacted] No other hostile activity has been reported. This investigation is being closed.

SECTION B – ENTITIES AND INDIVIDUALS

Name of Person: UNKNOWN
Title & Company: UNKNOWN & UNKNOWN
Role: Subject
Business Address: UNKNOWN,
Business Phone: UNKNOWN
EPA Employee: N

SECTION C – PROSECUTIVE STATUS

ADMIN/CRIMINAL/CIVIL ACTION(S): UNKNOWN
Investigation failed to identify individuals who penetrated the CSC (b) (7)(E) network and systems. No referral is made for action.

EXHIBITS

DESCRIPTION	EXHIBIT
EPA Form 2720-15 - Date Attached: 10/13/2009 Time Attached: 4:03:30...	1
EPA Form 2720-15 - Date Attached: 10/13/2009 Time Attached: 4:11:15...	2
EPA Form 2720-15 - Date Attached: 10/13/2009 Time Attached: 4:13:39...	3
EPA Form 2720-15 - Date Attached: 10/13/2009 Time Attached: 4:36:56...	4
EPA Form 2720-15 - Date Attached: 10/13/2009 Time Attached: 4:15:21...	5
EPA Form 2720-15 - Date Attached: 9/18/2009 Time Attached: 2:38:34 ...	6
EPA Form 2720-15 - Date Attached: 9/18/2009 Time Attached: 2:40:15 ...	7
EPA Form 2720-15 - Date Attached: 9/18/2009 Time Attached: 3:03:10 ...	8
(b) (7) (E) report	9
EPA Form 2720-15 - Date Attached: 10/7/2009 Time Attached: 3:47:19 ...	10
EPA Form 2720-15 - Date Attached: 10/7/2009 Time Attached: 3:58:40 ...	11
EPA Form 2720-15 - Date Attached: 10/7/2009 Time Attached: 4:00:46 ...	12
Tiger Documents 1	13

UNITED STATES ENVIRONMENTAL PROTECTION AGENCY
OFFICE OF THE INSPECTOR GENERAL
OFFICE OF INVESTIGATIONS
TWO POTOMAC YARD
2733 SOUTH CRYSTAL DRIVE
ARLINGTON, VA 22202

FINAL REPORT OF INVESTIGATION CONCERNING

UNKNOWN SUBJECT: UNAUTHORIZED ACCESS TO MULTIPLE EPA SERVERS (LAS VEGAS) OCI-AR-2011-CAC-2772

TABLE OF CONTENTS

Distribution:
File

Approvals:

_____
[redacted]
Senior Special Agent
Electronic Crimes Division

_____
[redacted]
Special Agent in Charge
Electronic Crimes Division

OFFICE OF INSPECTOR GENERAL
OFFICE OF INVESTIGATIONS

CASE NO.:	OCI-AR-2011-CAC-2772	**DATE OPENED:**	3/25/2011
CASE TITLE:	UNKNOWN SUBJECT: UNAUTHORIZED ACCESS TO MULTIPLE EPA SERVERS (LAS VEGAS)	**CASE AGENT:**	[redacted]
CASE CATEGORY:	COMPUTER INTRUSION	**OFFICE:**	OFFICE OF INVESTIGATIONS ELECTRONIC CRIMES DIVISION
JOINT AGENCIES:	None		
JURISDICTION:	NEVADA		

SECTION A - NARRATIVE

Predication

This investigation was opened on March, 25, 2011, The Office of Cyber Investigations and Homeland Security (OCI) received notification that suspicious network logins to EPA financial payment systems were occurring on several servers in Las Vegas, Nevada. The systems included in the reported suspicious activity were (b) (7)(E) [redacted]

Possible violations:

1. TITLE 18 USC SEC 1030, Fraud and related activity in connection with computers

Impact/Dollar Loss

This incident had the potential to impact all EPA financial systems and the physical security of environmental incident response and research facilities.

Synopsis

The investigation failed to determine the source of the unauthorized user account activity identified in the Las Vegas Finance center computer systems. Anomalies found in the system logs by EPA IT administrators compared with other available data failed to uncover the source or cause of the activity.

Forensic analysis of data available discovered an unidentified encrypted file that was unable to be opened for further analysis.

Details

Allegations: Violation of TITLE 18 United States Code Section 1030(a)-(4), Fraud and related activity in connection with computers, exceeding authorized access by a detailed Public Health Service employee

Allegations Findings: Investigation was unable to substantiate the allegation. No conclusive evidence of criminal activity could be determined.

Disposition

Due to the lack of conclusive evidence of criminal activity, no referral for prosecution or any course of legal action was made.

SECTION B – ENTITIES AND INDIVIDUALS

Name of Person: Unknown
Title & Company:
Role: Subject
Business Address:
Business Phone:
EPA Employee: N

SECTION C – PROSECUTIVE STATUS

ADMIN/CRIMINAL/CIVIL ACTION(S): NONE

EXHIBITS

DESCRIPTION	EXHIBIT
Memorandum of Activity for Imaging, Dated February 3, 2011	1
Memorandum of Interview for [redacted], Dated February 4, 2011	2
Memorandum of Activity for Network Monitoring, Dated February 5, 2011	3
Memorandum of Activity for Imaging, Dated February 5, 2011	4
Memorandum of Interview for [redacted] Dated September 21, 2011	5

UNITED STATES ENVIRONMENTAL PROTECTION AGENCY
OFFICE OF INSPECTOR GENERAL
TWO POTOMAC YARD
2733 SOUTH CRYSTAL DRIVE
ARLINGTON, VA 22202

CASE #: OCI-AR-2011-CAC-2783 **CROSS REFERENCE #:**

TITLE: Unknown Intrusion into EPA System (b) (7)(E)

CASE AGENT (if different from prepared by):

SHORT-FORM REPORT OF INVESTIGATION

PERIOD COVERED: FROM 4/15/2011 TO 1/10/2013

STATUS OF CASE: CLOSED INVESTIGATION

JOINT AGENCIES: None

DISTRIBUTION: SAC [redacted]
AIGI MICHAEL DAGGETT
File

PREDICATION: On April 11, 2011, the Office of Cyber Investigations and Homeland Security (OCI) discovered that an EPA system had been compromised by unknown individuals.

DETAILS: Due to the sensitive nature of the investigation, the details are not being reported in our electronic case management system. See the hard copy case file for the closing report of investigation.

Allegation 1: Title 18 USC SEC 1029 Fraud and related activity in connection with access devices.

Allegation 1 Findings: See hard copy case file

Allegation 2: Title 18 USC SEC 1030 Fraud and related activity in connection with computers.

Allegation 1 Findings: See hard copy case file

DISPOSITION: See hard copy case file

EXHIBITS: None

UNITED STATES ENVIRONMENTAL PROTECTION AGENCY
OFFICE OF THE INSPECTOR GENERAL
OFFICE OF INVESTIGATIONS
TWO POTOMAC YARD
2733 SOUTH CRYSTAL DRIVE
ARLINGTON, VA 22202

FINAL REPORT OF INVESTIGATION CONCERNING

UNKNOWN SUBJECT(S) – UNAUTHORIZED EPA LAN ACCESS
OCI-AR-2012-CAC-0014

TABLE OF CONTENTS

Distribution:
[redacted]
File

Approvals:

_____
Special Agent

_____
Special Agent in Charge

OFFICE OF INSPECTOR GENERAL
OFFICE OF INVESTIGATIONS

CASE NO.:	OCI-AR-2012-CAC-0014	**DATE OPENED:**	11/01/2011
CASE TITLE:	UNKNOWN SUBJECT(S) – UNAUTHORIZED EPA LAN ACCESS	**CASE AGENT:**	[redacted]
CASE CATEGORY:	COMPUTER INTRUSION	**OFFICE:**	OFFICE OF INVESTIGATIONS
JOINT AGENCIES:	None		
JURISDICTION:	DISTRICT OF COLUMBIA		

SECTION A - NARRATIVE

Predication

This investigation was opened on November 1, 2011, based on the notification by [redacted] Security Management Division, EPA, Washington, DC, of a security violation concerning EPA's Local Area Network committed by unknown person(s). According to [redacted] SMD was notified that unknown individual(s) were accessing EPA's LAN allegedly with a personal computer. The access was occurring in the EPA East and Ariel Rios North Buildings, Washington, DC. [redacted] related there have been at least six times the EPA LAN had been accessed so far.

Possible violations:

1. TITLE 18 USC SEC 1029, Fraud and related activity in connection with access devices

Impact/Dollar Loss

The impact of this incident represents a compromise of the command and control of EPA systems and the EPA network.

Synopsis

On November 1, 2011, [redacted], Security Management Division, EPA, Washington, DC reported a security violation concerning EPA's Local Area Network (LAN) committed by unknown person(s). According to [redacted], SMD was notified that unknown individual(s) were accessing EPA's LAN allegedly with a personal computer. The

access was occurring in the EPA East and Ariel Rios North Buildings, Washington, DC. [redacted] related there have been at least six times the EPA LAN had been accessed so far.

Although the allegations were substantiated as unauthorized access was documented in EPA's LAN records, the investigation was unable to positively identify the individual(s) who gained access to the EPA data networks through physical means to steal/maintain access to EPA internet resources. [redacted] (b) (7)(E)

Details

Allegation 1: 18 USC 1029 Fraud and related activity in connection with access devices.

Findings: Unknown individual(s), without proper authorization, gained access to the EPA physical LAN closets networks and utilized network resources.

Disposition

Investigation failed to identify the individual(s) who gained access to the EPA's network. No referral for prosecution was made.

SECTION B – ENTITIES AND INDIVIDUALS

Name of Person: Unknown
Title & Company:
Role: Subject
Business Address:
Business Phone:
EPA Employee: N

SECTION C – PROSECUTIVE STATUS

ADMIN/CRIMINAL/CIVIL ACTION(S): None

EXHIBITS

DESCRIPTION	EXHIBIT
MOI Interview of [redacted], August 24, 2011	1
MOI Interview of [redacted] September 6, 2011	2
MOI Interview of [redacted], October 28, 2011	3
MOA Review of Security Logs, February 9, 2012	4
MOA Attempt to contact [redacted], May, 30 2013	5

UNITED STATES ENVIRONMENTAL PROTECTION AGENCY
OFFICE OF INSPECTOR GENERAL
TWO POTOMAC YARD
2733 SOUTH CRYSTAL DRIVE
ARLINGTON, VA 22202

CASE #: OCI-AR-2012-CAC-0035 **CROSS REFERENCE #:**

TITLE: COMPROMISE OF EPA SYSTEMS (FO)

CASE AGENT (if different from prepared by):

SHORT-FORM REPORT OF INVESTIGATION

PERIOD COVERED: FROM 1/18/2012 TO 4/12/2013

STATUS OF CASE: CLOSED INVESTIGATION

JOINT AGENCIES: FBI

DISTRIBUTION: SAC [redacted]
AIGI MICHAEL DAGGETT
File

PREDICATION: On December 26, 2011, The Office of Cyber Investigations and Homeland Security (OCI) received notification from [redacted] Computer Security Incident Response Center (CSIRC), that EPA users had been compromised by navigating to foreign websites.

DETAILS: Due to the sensitive nature of the investigation, the details are not being reported in our electronic case management system. See the hard copy case file for the closing report of investigation.

Allegation 1: Title 18 USC SEC 1029 Fraud and related activity in connection with access devices.

Allegation 1 Findings: See hard copy case file

Allegation 2: Title 18 USC SEC 1030 Fraud and related activity in connection with computers.

Allegation 1 Findings: See hard copy case file

DISPOSITION: Investigation was not able to determine the identity of the intruders. A referral for prosecution was not made.

EXHIBITS: See hard copy case file

UNITED STATES ENVIRONMENTAL PROTECTION AGENCY
OFFICE OF INSPECTOR GENERAL

TWO POTOMAC YARD
2733 SOUTH CRYSTAL DRIVE
ARLINGTON, VA 22202

CASE #: OCI-AR-2012-CAC-0037 **CROSS REFERENCE #:**

TITLE: COMPROMISE OF EPA SYSTEMS (FO)

CASE AGENT (if different from prepared by):

SHORT-FORM REPORT OF INVESTIGATION

PERIOD COVERED: FROM 1/12/2012 TO 4/16/2013

STATUS OF CASE: CLOSED INVESTIGATION

JOINT AGENCIES: FBI

DISTRIBUTION: SAC [redacted]
AIGI MICHAEL DAGGETT
File

PREDICATION: On January 12, 2012, The Office of Cyber Investigations and Homeland Security (OCI) received notification from [redacted], EPA, Computer Incident Security Response Center (CSIRC), RTP, NC that an EPA system from Region 4 was suspected to have been compromised by Focused Operations (F0) (b) (7)(E) [redacted].

DETAILS: Due to the sensitive nature of the investigation, the details are not being reported in our electronic case management system. See the hard copy case file for the closing report of investigation.

Allegation 1: Title 18 USC SEC 1029 Fraud and related activity in connection with access devices.

Allegation 1 Findings: See hard copy case file

Allegation 2: Title 18 USC SEC 1030 Fraud and related activity in connection with computers.

Allegation 1 Findings: See hard copy case file

DISPOSITION: Investigation was not able to determine the identity of the intruders. A referral for prosecution was not made.

EXHIBITS: See hard copy case file

UNITED STATES ENVIRONMENTAL PROTECTION AGENCY
OFFICE OF INSPECTOR GENERAL
TWO POTOMAC YARD
2733 SOUTH CRYSTAL DRIVE
ARLINGTON, VA 22202

CASE #: OCI-AR-2012-CAC-0038 **CROSS REFERENCE #:**

TITLE: COMPROMISE OF EPA SYSTEMS (FO)

CASE AGENT (if different from prepared by):

SHORT-FORM REPORT OF INVESTIGATION

PERIOD COVERED: FROM 1/12/2012 TO 4/16/2013

STATUS OF CASE: CLOSED INVESTIGATION

JOINT AGENCIES: FBI

DISTRIBUTION: SAC [redacted]
AIGI MICHAEL DAGGETT
File

PREDICATION: On January 12, 2012, [redacted] Chief of Cyber Investigations, Office of Cyber Investigations and Homeland Security (OCI) received notification from [redacted] Computer Security Incident Response Center (CSIRC) that the US Computer Emergency Response Team (US-CERT) reported an EPA system located in RTP, NC had been compromised by Focused Operations (F0).

DETAILS: Due to the sensitive nature of the investigation, the details are not being reported in our electronic case management system. See the hard copy case file for the closing report of investigation.

Allegation 1: Title 18 USC SEC 1029 Fraud and related activity in connection with access devices.

Allegation 1 Findings: See hard copy case file

Allegation 2: Title 18 USC SEC 1030 Fraud and related activity in connection with computers.

Allegation 1 Findings: See hard copy case file

DISPOSITION: Investigation was not able to determine the identity of the intruders. A referral for prosecution was not made.

EXHIBITS: See hard copy case file

UNITED STATES ENVIRONMENTAL PROTECTION AGENCY
OFFICE OF INSPECTOR GENERAL

DATE: April 11, 2013 **PREPARED BY:** [redacted]

CASE #: OCI-AR-2012-CAC-0086 **CROSS REFERENCE #:**

TITLE: COMPRAMISE OF EPA NETWORK SECURITY

CASE CLOSING REPORT

Subject(s)	Location	Other Data
Unknown		

VIOLATION(S): Computer Intrusion

ALLEGATION: On April 2, 2012, the Environmental Protection Agency, Office of Inspector General, Office of Cyber Investigations and Homeland Security received notification from [redacted] EPA Computer Security Incident Response Center, RTP, NC, that numerous EPA systems were being targeted and compromised by unknown individuals and the computers were communicating to known malicious websites.

FINDINGS: Access to the EPA network was gained (b) (7)(E) [redacted]

[redacted] The network has been restored to a secure environment.

It was discovered that (b) (7)(E) [redacted]

As a precaution, the EPA notified anyone who's PII was contained in the documents and offered credit monitoring services (b) (7)(E) The PII breach team consisted of [redacted] The notifications were handled through the EPA National Privacy Program (http://[redacted](b) (7)(E)

The possible exposure of PII has been opened as a separate investigation (b) (7)(E)
(b) (7)(E) (b) (7)(E)

DISPOSITION: As the malware was removed, the network secured, no indication that data was removed and no reports of significant impacts to Agency operations, it is recommended that the investigation into the intrusion be closed. The Electronic Crimes Division will continue (b) (7)(E)

UNITED STATES ENVIRONMENTAL PROTECTION AGENCY
OFFICE OF THE INSPECTOR GENERAL
OFFICE OF INVESTIGATIONS
TWO POTOMAC YARD
2733 SOUTH CRYSTAL DRIVE
ARLINGTON, VA 22202

FINAL REPORT OF INVESTIGATION CONCERNING

SECURITY BREACH OF EPA MYPAY SYSTEM
OCI-AR-2012-CAC-0146

TABLE OF CONTENTS

Distribution:
File

Submitted By:

[redacted]
Special Agent
Electronic Crimes Division
Office of Investigations

Approved By:

[redacted]
Special Agent in Charge
Electronic Crimes Division
Office of Investigations

OFFICE OF INSPECTOR GENERAL
OFFICE OF INVESTIGATIONS

CASE NO.:	OCI-AR-2012-CAC-0146	**DATE OPENED:**	07/23/2012
CASE TITLE:	SECURITY BREACH OF EPA MYPAY SYSTEM	**LAST UPDATED:**	
CASE CATEGORY:	COMPUTER INTRUSION	**CASE AGENT:**	[redacted]
JOINT AGENCIES:	None	**OFFICE:**	OCI

JURISDICTION: VIRGINIA

SECTION A - NARRATIVE

Predication

An investigation was opened on July 23, 2012 based on information received from the Environmental Protection Agency (EPA), Computer Security Incident Response Center (CSIRC), Research Triangle Park, North Carolina. The investigation was initiated as a result of an EPA Employee alleging [redacted] MyPay account was potentially compromised.

Possible violations:

1. TITLE 18 USC SEC 1030, Fraud and related activity in connection with computers.
2. TITLE 18 USC SEC 1029, Fraud and related activity in connection with access devices.

Impact/Dollar Loss

No Dollar loss was sustained by the Government.

There were no impacts to EPA systems, programs, or processes.

Synopsis

On July 12, 2012, [redacted], CSIRC, Office of Environmental Information (OEI), EPA, Research Technology Park, North Carolina, notified [redacted], EPA Office of Inspector General (OIG), Office of Cyber Investigations (OCI), via email, of a reported security breach to an EPA employee's pay account on the EPA's MyPay System. The EPA employee, [redacted]

[redacted], EPA, Washington, DC, reported that an unauthorized change to [redacted] direct deposit designation was processed in the MyPay System.

This investigation disclosed the allegations were disproven. Investigative activities found there were, in fact, several changes made to [redacted] direct deposit account designation. The changes were made through standard procedures and protocol by [redacted] bank and the Defense Finance and Accounting Services (DFAS).

Details

Allegation: Violation of TITLE 18 United States Code Section 1030(a)(2), Fraud and related activity in connection with computers.

Violation of TITLE 18 United States Code 1029(a), Fraud and related activity in connection with access devices.

On July 20, 2012, [redacted] OCI, EPA,OIG, and [redacted] OCI, EPA, OIG, conducted an interview of [redacted] The purpose of this interview was to obtain information regarding the suspected security breach of [redacted] s MyPay account.

[redacted] stated [redacted] received a phone call on Tuesday, July 10, 2012 from [redacted] an employee of [redacted] bank [redacted] Federal Credit Union [redacted], who stated [redacted] federal direct deposit pay check was being directed to a nonexistent account (Account Number: [redacted]) within the same bank. [redacted] informed [redacted] did not make or authorize any changes to [redacted] direct deposit. Prior to ending the call, [redacted] created a new account for [redacted] and re-routed [redacted] direct deposit.

[redacted] contacted the Defense Finance and Accounting Services (DFAS) who informed [redacted] the change to the direct deposit account was made on July 3, 2012. Additionally, DFAS informed [redacted] the accounting logs showed three changes to [redacted] account; the first from [redacted] previous bank, the second to the invalid account, and the third to the new account created by [redacted] opined [redacted] had not logged into [redacted] MyPay account since July 3, 2012 but was sure [redacted] had made no changes to [redacted] direct deposit location. Furthermore, [redacted] does not remember when [redacted] last logged into MyPay. (EXHIBIT 1)

On July 20, 2012, [redacted] conducted a document review of email coordination between [redacted] and [redacted] DFAS, Customer Operations – MyPay, Finance Mission Area. The purpose of this document review was to determine DFAS' involvement in changing [redacted] federal direct deposit pay check.

On July 10, 2012, [redacted] sent an email to the CCL-MyPay-Project-Office organizational email address titled "MyPay Security Breach" wherein [redacted] reported a security breach of [redacted] MyPay account. [redacted] email stated [redacted] accessed MyPay and found the account

number for direct deposit had been changed. stated corrected the account number in MyPay and then contacted DFAS. The representative (spoke with informed that the "bogus change" was made on July 3, 2012. Furthermore, the representative stated there is a designation in the accounting system when an employee makes a change in MyPay. The representative stated they were able to determine that neither nor the EPA Personnel Office made the change, but could not determine who did.

On July 20, 2012, responded to email. stated the records showed direct deposit information was NOT changed using the MyPay system but was changed by civilian pay based on information received at DFAS. (EXHIBIT 2)

On July 25, 2012, interviewed DFAS, Customer Operations, Civilian Pay. confirmed the account in which federal pay check would be deposited into was changed by a DFAS, MyPay, Civilian Pay technician; however, (b) (6), (b) (7)(C), (b) (7)(E)

XHIBIT 3)

On September 24, 2012, conducted a telephonic interview of Federal Credit Union , Electronic/Optical Processing Loss Prevention Officer. looked into the allegation and came to the conclusion there was a mistake made by (b) (6), (b) (7)(C), (b) (7)(E)

(EXHIBIT 4)

Disposition

This investigation disclosed all allegations were disproven and no criminal activity occurred. There were no attempts to defraud the government or government employees and there were no connected security breaches to the EPA MyPay System.

SECTION B – ENTITIES AND INDIVIDUALS

Name: [redacted]
Role: Victim
EPA Employee: Y
Business Address: Ariel Rios South, Room [redacted] 1200 Pennsylvania Avenue, N.W., Washington, DC 20406
Business Phone: 202[redacted]

SECTION C – PROSECUTION STATUS

ADMIN/CRIMINAL/CIVIL ACTION(S): As the allegation was disproven and no criminal activity was identified this case was not referred for action.

EXHIBITS

DESCRIPTION	EXHIBIT
MOI-07/26/2012 – [redacted]	1
MOA-07/24/2012 – [redacted]: Email to DFAS [redacted]	2
MOI-07/26/2012 – [redacted]	3
MOI – 10/09/2012 – [redacted] and [redacted]	4

UNITED STATES ENVIRONMENTAL PROTECTION AGENCY
OFFICE OF THE INSPECTOR GENERAL
OFFICE OF INVESTIGATIONS
TWO POTOMAC YARD
2733 SOUTH CRYSTAL DRIVE
ARLINGTON, VA 22202

FINAL REPORT OF INVESTIGATION CONCERNING

BREACH OF REGION[redacted] SERVER
OCI-AR-2012-CAC-0147

TABLE OF CONTENTS

Distribution:
File

Submitted By:

[redacted]
Special Agent
Electronic Crimes Division
Office of Investigations

Approved By:

[redacted]
Special Agent in Charge
Electronic Crimes Division
Office of Investigations

OFFICE OF INSPECTOR GENERAL
OFFICE OF INVESTIGATIONS

CASE NO.:	OCI-AR-2012-CAC-0147	**DATE OPENED:**	07/25/2012
CASE TITLE:	BREACH OF REGION [redacted] SERVER	**LAST UPDATED:**	
CASE CATEGORY:	COMPUTER INTRUSION	**CASE AGENT:**	[redacted]
JOINT AGENCIES:	None	**OFFICE:**	ECD

JURISDICTION: [redacted]

SECTION A - NARRATIVE

Predication

An investigation was opened on July 25, 2012, based on information received from the Environmental Protection Agency, Computer Security Incident Response Center, Research Triangle Park, North Carolina. The investigation was initiated as a result of an EPA Information Security Officer reporting a breach of security resulting in unauthorized changes being made to a Region [redacted] server.

Possible violations:

TITLE 18 USC SEC 1030, Fraud and related activity in connection with computers.

Impact/Dollar Loss

No Dollar loss was sustained by the Government.

There were no significant impacts to EPA systems, programs, or processes.

Synopsis

On March 6, 2012, [redacted], CSIRC, Office of Environmental Information, EPA, Research Triangle Park, North Carolina, notified [redacted], EPA, Office of Inspector General, Office of Investigations, Electronic Crimes Division, of the possible breach of an EPA Region [redacted] server by an unidentified person. Specifically, the breach consisted of unauthorized changes being made to the Region [redacted] server.

This investigation disclosed the allegations were proven. Investigative activities found there were, in fact, changes made to the server's desktop background. However, the investigation found no criminal activity or malicious intent related to this incident.

Details

Allegation: Violation of TITLE 18 United States Code Section 1030(a)(5), Fraud and related activity in connection with computers.

On March 9, 2012, [redacted] and [redacted], EPA, OIG, OI, Denver Field Office, interviewed [redacted] EPA, Region [redacted] Technical Services Unit, [redacted] verified the details of the allegation regarding the suspected breach of the server in question. They confirmed unauthorized changes were made to a virtual server image which was used to image employee computers in the Region. [redacted] stated [redacted] the last known good deployment of the image from this server sometime around noon on March 5, 2012. Based on this, [redacted] believed the compromise occurred sometime after 1 p.m. on March 5, 2012.

[redacted] stated [redacted] discovered that when attempting to load an image from the virtual server to a local computer, a background image was displayed during the boot loader process. This image depicted a cartoon [redacted] Normally, the Microsoft logo would be displayed during this process.

[redacted] opined, after considering the totality of the circumstances involved, it would be a "virtual impossibility" that the server image was compromised from outside of EPA. [redacted] conducted a review of the server's access authorities and discovered [redacted] contractors, [redacted] Silver Spring, Maryland, had user rights to the database. A review of the server's internal logs by [redacted] disclosed that [redacted] along with [redacted] contractors [redacted] were active on the system during the time of the incident. Based on this review, [redacted] stated [redacted] specifically suspected [redacted] was responsible for the change made to the server. [redacted] was unable to say definitively from [redacted] examination of the logs that [redacted] was involved with the incident; only that [redacted] had a "gut-feeling." [redacted] offered no other support for this conclusion. (EXHIBIT 1)

On January, 29, 2013, [redacted], EPA, OIG, OI, ECD, conducted an interview of [redacted], contractor, [redacted] stated [redacted] is the [redacted] for the contract responsible for supporting the Region [redacted] Technical Services Unit. During February or March 2012, [redacted] and [redacted] of contractors were tasked with creating a Microsoft Deployment Toolkit (MDT) server which was to be used to deploy Windows 7 operating systems to customers located in Region [redacted] team, responsible for building and testing the server, consisted of [redacted], [redacted]. [redacted] stated the individuals on [redacted] team were the only persons with initial access to the server. However, during March 2012, [redacted] and [redacted]

provided their EPA government employee counterparts with a demonstration of the server's capabilities. Shortly after the demonstration (NFI), the following EPA government employees requested and were granted access to the server: [redacted] Information Technology Specialists, EPA, Region [redacted], and [redacted] stated, to the best of [redacted] recollection, a "day or two" after the EPA government employees were granted access to the server, a change was made to the servers background. [redacted] could not recall what changes were made to the server; however, [redacted] did recall there were no significant impacts to operations and opined no one [redacted] was responsible. (EXHIBIT 2)

On January 29, 2013, [redacted] conducted an interview of [redacted] recalled [redacted] being tasked to create a MDT server which would be used in deploying Windows 7 operating system images to Region [redacted] customers. [redacted] stated [redacted] did not have the same level of involvement during this project as others on [redacted] did. [redacted] relayed [redacted] and [redacted] were the main team members to develop and use the MDT server. [redacted] further stated two government employees, [redacted] and [redacted] also had access to the server. [redacted] opined the [redacted] individuals most likely to make the changes to the server were [redacted] due to their sense of humor. However, [redacted] could not definitively say who had made the changes to the server. (EXHIBIT 3)

On January 29, 2013, [redacted] conducted an interview of [redacted] recalled that sometime in March 2012 [redacted] tasked the contracting team with developing a new MDT server. [redacted] stated [redacted] discussed this project with [redacted] who then set up access to the server. Initially, the contractors were the only individuals with access to the server. [redacted] stated during this time, [redacted] had changed the background on the server to depict a cartoon image [redacted] Shortly after this change was made, the government requested access to the server. Because government employees requested access, [redacted] removed the cartoon image on the server and restored the original background.

A couple of weeks after the government employees received access to the MDT server, [redacted] noticed the background on the server was changed to a cartoon image [redacted] Upon noticing the change, [redacted] called [redacted] and asked if [redacted] had made a change to the server; [redacted] replied "no."

[redacted] stated multiple government employees had access to the server and they utilized the same username, [redacted] and password so there was no way to determine exactly which government employees had access to the server.

In addition, [redacted] stated [redacted] believed [redacted] may have made the changes to the server and is now trying to place the blame on [redacted] [redacted] stated [redacted] has "a problem" with [redacted] doesn't do things the way [redacted] wants. (EXHIBIT 4)

On January 29, 2013, [redacted] conducted an interview of [redacted] stated, during February or March of 2012, a team of contractors with [redacted] Inc., set up a MDT server in order to push images to Region [redacted] customers. [redacted] stated

[redacted] and [redacted] other contractors (NFI) knew how to use the MDT server and were very familiar with the system. [redacted] stated [redacted] built the system and would likely have known how to make changes to the server. [redacted] believed the change made to the server background was nothing more than a joke which had been blown out of proportion. Additionally, [redacted] stated the server in question is not in use anymore because it was only used to deploy Windows XP images, which is no longer used by Region [redacted] Furthermore, [redacted] stated that at the time of the incident [redacted]. contractors were the only individuals with access to the server; however, at some point, government employees were give access to the server. [redacted] believes if anyone would have made the changes to the server it would have been [redacted] (EXHIBIT 5)

On January 30, 2013, [redacted] conducted an interview of [redacted] [redacted] could not recall when [redacted] was made aware of the incident; however, [redacted] stated it was shortly after the incident occurred. [redacted] stated [redacted] did not believe the changes to the server were made intentionally or maliciously. [redacted] believed [redacted] [redacted] contractor, [redacted] [redacted]., would have been the individual most likely to make the changes due to [redacted] humorous nature. Additionally, [redacted] opined the incident was "no big deal" as there was no damage done to the server. (EXHIBIT 6)

On January 30, 2013, [redacted] conducted an interview of [redacted] During February or March 2012, [redacted] was made aware of an incident involving a MDT server. [redacted] stated someone had changed the background of the server. When an IT Specialist would begin imaging machines remotely, an image would pop up in the background. [redacted] stated when this incident occurred the affected server was in a "testing" phase and was not used in live operations. [redacted] stated [redacted] believed there were some configuration changes making the server unable to deploy software.

[redacted] opined the [redacted] contractors most likely made the changes to the server. [redacted] believes this because the contractors initially configured the server and possessed the most knowledge of the server's operational capabilities. Furthermore, [redacted] staff of government employees took over the development and use of the MDT server which may have caused the contractors to feel threatened. (EXHIBIT 7)

On January 30, 2013, [redacted] conducted an interview of [redacted] During February or March 2012, [redacted] was made aware of an incident involving a MDT server. [redacted] recalled receiving a phone call from [redacted] asking if [redacted] made any changes to the MDT server. [redacted] told [redacted] he had not made any changes to the MDT server. [redacted] described the image to [redacted] stated [redacted] believed [redacted] knew what image [redacted] was referring to. [redacted] has changed the background view on the MDT client only [redacted] sees on [redacted] computer; however, it shouldn't have been seen by anyone else. [redacted] provided [redacted] with a printed image that matched the description of the posting made to the server. [redacted] stated [redacted] remembered using this image as [redacted] background at some point but stated [redacted] never intentionally used this image as a background other users would see. [redacted] stated it is possible [redacted] was logged into the MDT server on [redacted] government issued computer and mistakenly changed the background on the MDT server while intending to make the change to [redacted] personal background view.

[redacted] explained that during the course of [redacted] work [redacted] has multiple processes running on [redacted] government issued computer. [redacted] stated if [redacted] was conducting work on the MDT through the MDT application on [redacted] government issued computer [redacted] could have accidentally changed the background on the MDT application rather than [redacted] desktop. [redacted] maintained this was not intentional. (EXHIBIT 8)

Disposition

This investigation disclosed the allegation was proven; however, no criminal or malicious activities were found to have occurred to intrude upon, breach security within, or compromise EPA systems.

SECTION B – ENTITIES AND INDIVIDUALS

Name: [redacted]
Role: Subject
EPA Employee: N
Business Address: [redacted]
Business Phone: [redacted]

SECTION C – PROSECUTION STATUS

ADMIN/CRIMINAL/CIVIL ACTION(S): As there was no criminal activity discovered during this investigation this case was not referred for action.

EXHIBITS

DESCRIPTION	EXHIBIT
MOI-03/09/2012 – [redacted]	1
MOI-01/29/2013 – [redacted]	2
MOI-01/29/2013 – [redacted]	3
MOI-01/29/2013 – [redacted]	4
MOI-01/29/2013 – [redacted]	5
MOI-01/30/2013 – [redacted]	6
MOI-01/30/2013 – [redacted]	7
MOI-01/30/2013 – [redacted]	8

UNITED STATES ENVIRONMENTAL PROTECTION AGENCY
OFFICE OF INSPECTOR GENERAL

DATE: July 24, 2013 **PREPARED BY:** [redacted]

CASE #: OCI-AR-2012-CAC-0153 **CROSS REFERENCE #:**

TITLE: UNNKNOWN SUBJECT: EXPOSURE OF PII DATA IN CONNECTION TO EPA NETWORK INTRUSION

CASE CLOSING REPORT

Subject(s)	Location	Other Data
Unknown		

VIOLATION(S): Computer Intrusion

ALLEGATION: On April 2, 2012, The Office of Cyber Investigations and Homeland Security (OCI) received notification from [redacted] EPA Computer Security Incident Response Center (CSIRC), RTP, NC, that numerous EPA systems were being targeted and compromised by unknown individuals and that the systems were communicating to known malicious websites. Personally Identifiable Information (PII) was resident on one of the compromised servers and it was feared the PII could have been compromised.

FINDINGS: Access to the EPA network was gained (b) (7)(E) [redacted]

[redacted]

It was discovered that (b) (7)(E) [redacted]

(b) (7)(E) [redacted]

As a precaution, the EPA notified anyone who's PII was contained in the documents and offered credit monitoring services. The PII breach team consisted of [redacted] and [redacted] The notifications were handled through the EPA National Privacy Program (http:/[redacted]

A total of approximately (b) (7)(E) [redacted] employees notified accepted the offer of credit monitoring. To date none of those (b) [redacted] employees have reported any anomalies or suspect transactions or information on their credit report.

DISPOSITION: It is recommended that the investigation into the possible theft of PII be closed. After over one year of credit monitoring services no employee has been subjected to any suspicious activity. (b) (7)(E) [redacted]

UNITED STATES ENVIRONMENTAL PROTECTION AGENCY
OFFICE OF INSPECTOR GENERAL

1301 CONSTITUTION AVE., NW
WASHINGTON, DC 20004

DATE: MAY 31, 2013 **PREPARED BY:** [redacted]

CASE #: OCI-HQ-2011-CAC-1229 **CROSS REFERENCE #:**

TITLE: UNAUTHORIZED ACCESS TO GOVERNMENT SYSTEMS

COMPLAINT SUMMARY REPORT

Subject(s)	Location	Other Data
Unknown		

COMPLAINT: On December 6, 2010, The Office of Cyber Investigations and Homeland Security received notification that (b) (7)(E) [redacted] detected by the US Computer Emergency Response Team that contained EPA domain information and email pertaining to an EPA contractor.

On December 6, 2010, [redacted] interviewed [redacted] Computer Sciences Corporation, RTP, NC. OCI [redacted] interviewed [redacted] as part of a network intrusion investigation related to [redacted] home computer being compromised. A keylogger had been detected by the US CERT that contained EPA data and reported to the Agency.

[redacted] related [redacted] had been notified by the EPA's CSIRC on December 3, 2010 and told that all [redacted] accounts, except webmail, had been suspended after receiving information they may be compromised by malware. [redacted] related [redacted] was told the details and conducted some steps to try and detect the malware on [redacted] system. [redacted] related [redacted] scanned [redacted] system with Malware Bytes and a few other malware detection tools which discovered multiple files. [redacted] related that [redacted] had (b) (7)(E) [redacted] from the internet in the past 30 days.

INVESTIGATIVE FINDINGS: Initial investigation by the US CERT and forensic analysis revealed (b) (7)(E), (b) (7)(C), (b) (6) [redacted] other pieces of malware were identified and resident on [redacted] computer as well as numerous other suspicious files that were password protected.

Investigation revealed that [redacted] had been using a computer that was infected with multiple pieces of malicious software. (b) (7)(E) [redacted] had been partially removed and rendered inoperative.

RECOMMENDATION: (b) (5) [redacted]

this investigation should be closed. The threat to the EPA has been mitigated and further analysis of malware discovered would be an inefficient use of limited resources.

UNITED STATES ENVIRONMENTAL PROTECTION AGENCY
OFFICE OF THE INSPECTOR GENERAL
OFFICE OF INVESTIGATIONS
TWO POTOMAC YARD
2733 SOUTH CRYSTAL DRIVE
ARLINGTON, VA 22202

FINAL REPORT OF INVESTIGATION CONCERNING

UNKNOWN SUBJECT: INTRUSIONINTO MULTIPLE WORKSTATIONS (b) (7)(E) AND (b) (7)(E)

OCI-RTP-2012-CAC-0062

TABLE OF CONTENTS

Distribution:
[redacted]
SAC
File

Approvals:

_____
Special Agent

_____
Special Agent in Charge

OFFICE OF INSPECTOR GENERAL
OFFICE OF INVESTIGATIONS

CASE NO.:	OCI-AR-2012-CAC-0062	**DATE OPENED:**	02/24/2012
CASE TITLE:	UNKNOWN SUBJECT: INTRUSIONINTO MULTIPLE WORKSTATIONS (b) (7)(E) [redacted]	**CASE AGENT:**	[redacted]
CASE CATEGORY:	COMPUTER INTRUSION	**OFFICE:**	OFFICE OF CYBER INVESTIGATIONS AND HOMELAND SECURITY - IMMEDIATE OFFICE
JOINT AGENCIES:	Federal Bureau of Investigation		
JURISDICTION:	N/A		

SECTION A - NARRATIVE

Predication

On February 16, 2012, Special Agent [redacted], United States Environment Protection Agency, Office of Inspector General, Office of Investigations, Region 4, Research Triangle Park field office, received a complaint from [redacted] Office of Technology Operations and Planning, and Technology Information Security Staff, [redacted], pertaining to an intrusion of the Office of the Administrator, [redacted] computer, and the Office of Air and Radiation, [redacted] computer.

Possible violations:

1. TITLE 18 USC SEC 1029, Fraud and related activity in connection with access devices
2. TITLE 18 USC SEC 1030, Fraud and related activity in connection with computers

Impact/Dollar Loss

This incident impacted the security and stability of the EPA local area network and EPA Senior Level administration operations.

Synopsis

On February 16, 2012, Special Agent [redacted] United States Environment Protection Agency, Office of Inspector General, Office of Investigations, Region [redacted] field office, received a complaint from [redacted] Office of Technology Operations and Planning, and Technology Information Security Staff, [redacted], pertaining to an intrusion of the Office of the Administrator, [redacted] computer, and the Office of Air and Radiation, [redacted] computer. (Exhibit 1)

On February 20, 2012 [redacted], OCI coordinated with the Cyber division of the Federal Bureau of Investigation who offered to assist with any information they had related to the intrusion but declined to join this investigation.

On February 22, 2012 analysis was completed (b) (7)(E) malware recovered from the intrusion incident by the CSIRC. Analysis showed the malware was fairly common and targeted a wide audience of recipients. (Exhibit 2)

On January 30, 2013 [redacted], OCI, interviewed [redacted] and discussed [redacted] position and activities in OA. [redacted] was unsure how [redacted] system had been compromised or why [redacted] would have been targeted. (Exhibit 3)

Details

Allegation 1: Title 18 USC SEC 1029 Fraud and related activity in connection with access devices.

Findings: On February 16, 2012, TISS reported EPA systems (b) (7)(E) [redacted] no damage was discovered to the EPA network. No additional information was available to identify the intruders.

Allegation 2: Title 18 USC SEC 1030 Fraud and related activity in connection with computers.

Findings: On February 16, 2012, TISS reported (b) (7)(E) [redacted] no damage was discovered to the EPA network. No additional information was available to identify the intruders.

Disposition

Investigation was not able to determine the identity of the intruders. A referral for prosecution was not made.

SECTION B – ENTITIES AND INDIVIDUALS

Name of Person: Unknown
Title & Company:
Role: Subject
Business Address:
Business Phone:
EPA Employee: N

SECTION C – PROSECUTIVE STATUS

ADMIN/CRIMINAL/CIVIL ACTION(S): None

EXHIBITS

DESCRIPTION	EXHIBIT
Case Initiation	1
MOA Malware Analysis	2
MOI Interview of [redacted]	3

UNITED STATES ENVIRONMENTAL PROTECTION AGENCY
OFFICE OF INSPECTOR GENERAL

DATE: September 13, 2013 **PREPARED BY:** [redacted]

CASE #: OI-HQ-2013-CAC-0091 **CROSS REFERENCE #:**

TITLE: COMPROMISE OF WWW.[redacted] GOV WEBSITE SERVERS

CASE CLOSING REPORT

Subject(s)	Location	Other Data
UNKNOWN	[redacted]	

VIOLATION(S): 18 USC § 1030 - FRAUD AND RELATED ACTIVITY IN CONNECTION WITH COMPUTERS

ALLEGATION: The Environmental Protection Agency, Office of Inspector General, Office of Investigations, Electronic Crimes Division, received information that the www[redacted] ov website servers had been compromised on April 30, 2013. The website is externally hosted by [redacted].

The website had to be taken off line for several days while triaged and analyzed.[redacted]

FINDINGS: ECD made arrangements to image the servers and to provide copies to CSIRC for analysis. It was determined that [redacted] www [redacted] gov. [redacted]

[redacted]

[redacted]

[redacted] registered to VLPS, Inc. 1744 West Katella Avenue, Suite 200, Orange, CA 92867 (http://www.vpls.net/profile/). VLPS is a hosting and support company specializing in virtual and cloud computing. VLPS has facilities in California and Virginia. The American

Registry for Internet Numbers (ARIN) indicates that this IP address is allocated to the Asian Pacific Network Information Centre (APNIC) and is registered in Thailand.

(b) (7)(E) is registered to Ubiquity Server Solutions, 12101 Tukwila International Blvd., Tukwila, WA 98168 (https://www.ubiquityservers.com/seattle-data-center). Ubiquity is a server hosting company providing dedicated and cloud computing, the Seattle data center provides service for the Western United States, Canada, and Asia.

(b) (7)(E) is registered to Pacific Internet, Taikoo Shing, Island East, Hong Kong (www.Pacnet.com). Pacnet owns and operates complete network systems throughout Asia, including data hosting and servicing.

Forensic analysis also identified one destination where it looked lik (b) (7)(E)

(b) (7)(E) is owned by AT&T Internet Services, 2701 N. Central Expressway, Richardson, TX, 75080, and is a "Direct Allocation." According to AT&T the designation as "Direct Allocation" indicates the server is wholly controlled by a separate entity. An IG subpoena was issued to AT&T Internet Services to determine ownership of the destination server.

An email response was delivered on June 28, 2013 in response to an Inspector General subpoena issued to AT&T Internet Services, Legal Compliance Group, 1010 N. St. Mary's Street, Room 315-A2, San Antonio, TX 78215, Fax (707) 435-6409, served on June 18, 2013. The response indicated that AT&T had no records pertaining to IP address (b) (7)(E)

Further research identified the IP address belongs to a sub-division of AT&T. According to the Domain Dossier service, the Registrant is SBC Internet Service, Inc., 12976 Hollenberg Drive, Bridgeton, MO 63044 and the administrative contact is .

AT&T Internet Services Compliance Officer, confirmed that information regarding the IP address was not available because AT&T Internet Services has no record of this IP address having been assigned/provisioned to any subscriber. The only record(s) regarding this IP address are that it appears to have been staged for future provisioning for AT&T U-verse subscribers.

Inquiries with other cyber law enforcement and intelligence agencies did not provide any viable leads or indication that information was exfiltrated from the (b) (7)(E)

DISPOSITION: It is recommended this case be closed due to lack of investigative leads, no confirmation that data was exfiltrated and the probability that further investigation will be not produce results.

UNITED STATES ENVIRONMENTAL PROTECTION AGENCY
OFFICE OF INSPECTOR GENERAL

DATE: February 8, 2013 **PREPARED BY: SA [redacted]**

CASE #: OI-AR-2012-CAC-0206 **CROSS REFERENCE #:**

TITLE: UNAUTHORIZED USE OF EPA CREDENTIALS / MISREPRESENTATION OF GOVERNMENT OFFICIAL

CASE CLOSING REPORT

Subject(s)	Location	Other Data
UNSUB	UNKNOWN	

VIOLATION(S):

NONE

ALLEGATION:

NONE

FINDINGS:

NONE

DISPOSITION:

Administratively closed. Two case numbers inadvertently assigned to one incident in IGEMS.

For additional information pertaining to this investigation, please refer to EPA OIG Case #:

OI-AR-2012-CAC-0207

UNAUTHORIZED USE OF EPA CREDENTIALS / MISREPRESENTATION OF GOVERNMENT OFFICIAL

UNITED STATES ENVIRONMENTAL PROTECTION AGENCY
OFFICE OF INSPECTOR GENERAL
OFFICE OF INVESTIGATIONS

1595 WYNKOOP STREET, 4th FLOOR
DENVER, CO 80202

DATE: March 19, 2013 **PREPARED BY:** [redacted]

CASE #: 2009-CS-0085 **CROSS REFERENCE #:**

TITLE: LIBBY SUPERFUND SITE

CASE CLOSING REPORT

Subject(s)	Location	Other Data
Unknown	Libby, Montana EPA Region 8, Denver, Colorado EPA Headquarters, Washington, D.C.	

VIOLATION(S):

18 U.S.C. § 242 (Deprivation of Right Under Color of Law)
18 U.S.C. § 371 (Conspiracy to Commit Offense or to Defraud the United States)
18 U.S.C. § 1001 (False Statements)
18 U.S.C. § 1341 (Mail Fraud)
18 U.S.C. § 1343 (Wire Fraud)
18 U.S.C. § 1346 (Scheme or Artifice to Defraud [Honest Services])

ALLEGATION: An allegation was received that unknown EPA officials violated the civil rights of the citizens of Libby, Montana, by not performing required scientific testing to determine the safe expose level to Libby amphibole asbestos; released written information to the public stating their homes were safe when they (unknown EPA officials) knew the homes could still be contaminated and present a danger to the citizens of Libby; and EPA officials failed to provide honest services to the citizens of Libby, Montana, in the clean-up of asbestos from the W.R. Grace mine that may have contaminated the town of Libby, Montana.

FINDINGS: Interviews of EPA personnel (to include EPA scientists) and hundreds of residents of Libby, Montana; and a review of documentation associated with the allegations in question were conducted. The investigation demonstrated that the EPA proceeded in the clean-up of attic insulation under an Emergency Response Removal Action (ERRA) in violation of the requirements of the Comprehensive Environmental Response, Compensation and Liability Act (CERCLA) and proceeded to perform remediation activities without conducting the required Baseline Risk Assessment.

During the conduct of the ERRA, it was determined that attic insulation contained within homes in Libby, Montana, as well as an innumerable quantity of homes located throughout the United States, may provide a substantial risk of endangerment to citizens. The EPA On-Scene Coordinator (OSC) determined, along with EPA officials, that removal of the attic insulation within Libby, Montana, was imperative to reduce the public health risk. However, CERCLA prohibits the removal of "product" where the "product" is contained within the structure unless there is a declaration of a Public Health Emergency (PHE). (b) (5) , EPA officials in concert with officials at the Office of Management and Budget, made the decision to remove attic insulation and by-pass CERCLA prohibitions by determining the insulation was a "non-product", (b) (5)

DISPOSITION: This investigation was referred to the United States Attorney's Office (USAO) in Great Falls, Montana, for possible criminal prosecution. The USAO declined prosecution based on (b) (5)

All actions and remedies have been addressed, and no further investigative activity is warranted. This case is closed.